THE 2001 CAPE TOWN CONVENTION
ON INTERNATIONAL INTERESTS IN MOBILE EQUIPMENT

RAIL WORKING GROUP

An association under Swiss law

www.railworkinggroup.org

Baarerstrasse 96, PO Box 7262, 6302 Zug, Switzerland
Tel: +41 (0)41 760 28 88; email: info@railworkinggroup.org

RailWorkingGrp
LinkedIn

An Introduction to the Luhn Algorithm

The Luhn Algorithm is named after its German creator, computer science researcher Hans Peter Luhn. It is a simple check digit formula used very widely to validate ID numbers. Its proven scope of applications is very broad:[1]

- Credit card numbers
  - Including VISA, AMEX, Mastercard, Diners Club, etc.
- US National Provider IDs, issued to healthcare providers
- Canadian + Greek social insurance numbers
- Israeli + South African national ID numbers
- Survey codes appearing on receipts of major restaurant chains
  - Including McDonalds, Taco Bell, etc.

The algorithm is in the public domain and is specified in ISO/IEC 7812. Unlike more sophisticated, proprietary security techniques, the Luhn Algorithm's purpose is not to guard against malicious hackers. Instead, the Luhn Algorithm is employed as a simple method to distinguish valid numbers from invalid ones, such as those corrupted by typos.

How does it work?

Take the number 12345674; let us assume it is a valid credit card number. The final digit (4) is a kind of control key (also called check digit) to analyse the integrity of the remaining digits. If two of the initial numbers (for example, producing 1324567 instead of 1234567) are scrambled and entered into the Luhn Algorithm, a result other than 4 will be generated, proving the invalidity of the number.

[1] https://www.geeksforgeeks.org/luhn-algorithm/

A closer look at the maths behind these validity checks

The Luhn Algorithm starts at the end of the number, from the last right digit to the first left digit. One must multiply by 2 all digits of even rank, going from left to right as aforementioned. If the double of a digit is equal or superior to 10, replace it by the sum of its digits. The find the sum ***s*** of all digits found. The control digit ***c*** is equal to ***c***=(10−(***s***mod10)mod10). (A friendly reminder: mod refers to the modulo operation. Modulo is the name of the calculus of the remainder in the Euclidean division. The modulo calculator returns the rest of the integer division.)

A concrete example using the formula[2]

- The number 853X, please find the check digit X.
- Take the digit 3, double it, 3*2 = 6.
- Take the digit 5, do not multiply by 2.
- Take the 8, multiply by 2: 8*2=16 and due to it being greater than 10, find the sum of its digits: 1+6=7
- The sum ***s*** is 6+5+7 = 18. As 18 mod 10 = 8, the final calculation yields
- c = (10 – 8mod10) = (10-8) = 2
- 2 is the check digit and 8532 is therefore valid according to Luhn.

Here is a graph to further visualize this example:

8	5	3	0
8*2=16	Stays 5	3*2=6	Stays 0
1+6=7	5	6	0
s=7	+5	+6	+0=18
			c=10-((18mod10)mod10) c=10-(8mod10) c=10-8 c=2

[2] https://www.dcode.fr/luhn-algorithm

Conclusion

The Luhn Algorithm is an effective, publicly available means of checking the validity of numbers. It cannot guard against malicious attacks, nor is it used by banks to calculate their Card Validation Codes. Furthermore, the Luhn Algorithm cannot check the validity of dates on cards.[3]

The Luhn algorithm will however detect any single-digit error, as well as almost all transpositions of adjacent digits. It does however have some flaws:

1. It will not detect transposition of the two-digit sequence 09 to 90 (or vice versa).[4]

2. It will detect most of the possible twin errors (but it will not detect 22 ↔ 55, 33 ↔ 66 or 44 ↔ 77).[5]

More complex and secure algorithms (ex. Verhoeff Algorithm) exist but their commercial use is comparatively quite limited; they simply lack the convenience (especially from a computing and management perspective) that the Luhn Algorithm, which as demonstrated above can be employed with mere pen-and-paper, can offer solutions to all sorts of issuers of important numbers.

For more on the Luxembourg Rail Protocol, visit www.railworkinggroup.org., as well as the UNIDROIT website www.unidroit.org. Keep up to date with all the latest developments via the Rail Working Group's LinkedIn group page.

[3] https://www.investopedia.com/terms/l/luhn-algorithm.asp
[4] https://planetcalc.com/2464/
[5] Kamaku and Wachira, Twin Error Detection in Luhn's Algorithm (2015)